Financial Information Security

James M. Brundy

San Diego, California

January 19, 2002

I. Managing Risks From "Networked Processing"

- Risks of using Internet and 3rd-party service providers; Protection of customer information
- Regulatory direction to banks on these subjects.
- Applies generally to using networks to process sensitive data

Risks of the Internet

- Internet networked workstations/servers contain security lapses.
- World Wide Web browsers attacked by viruses, trojan horses, etc.
- User of Internet as its network with suppliers/servicers/customers must address the security issues.
- Additional risks from using “start-ups.”

Risks of Using 3rd-Party Service Providers

- **Strategic** - Inappropriate business model or improper implementation.
- **Reputation** - Adverse public opinion due to 3rd-party acts/omissions.
- **Compliance** - Violation or law or regulation or nonconformity with **FI**'s policies, procedures or ethical standards.

Risks of Using 3rd-Party Service Providers (cont'd)

- **Transaction** - problems with service delivery; processing errors.
- **Credit** - 3rd party's failure to perform as agreed.
- **Country Risk** & other aspects of use of out-of-country service provider**.**

II. Risk Management Process for 3rd-Party Service Providers

- Risk assessment and strategic planning for use of 3rd parties by senior management and Directorate
- Due diligence in selecting each 3rd-party – qualitative and quantitative aspects

Risk Management Process for 3rd-Party Service Providers (cont'd)

- Require written contracts clearly specifying rights and responsibilities; prepared or reviewed by attorneys
- Oversee ongoing relationship; monitor and document oversight program

Implications

- Require in-house expertise and assigned personnel to manage 3rd-party arrangements
- Need policies and procedures for use of Internet-based network and for use of 3rd-party service providers
- Use of experienced counsel (typically external) to prepare contracts.

Example - Weblinking

- The OCC applied these risk management process in its guidance on weblinking: Banks must

1. Conduct sufficient due diligence on proposed linking partners' ability to provide service and maintain information security and privacy policies to minimize strategic and reputation risk.

Example - Weblinking (cont'd)

2. Negotiate formal contracts defining the rights and responsibilities to minimize transaction and reputation risk.
3. Display appropriate disclosures on the Bank's website to avoid customer confusion about who provides the services, in order to minimize transaction and compliance risk.

III. Protection of Customer Information

- Gramm-Leach-Bliley Act required **FI** agencies to establish standards to:
  - insure the security and confidentiality of customer … information
  - protect against … threats or hazards to [its] security or integrity
  - protect against unauthorized access or use

Protection of Customer Information (cont'd)

- Regulatory Guidelines require each **FI** to
  - Implement a comprehensive information security program covering all consumer customer information in electronic or paper form.
  - Involve the Board in oversight of the program, including assigning implementation responsibility and reviewing management reports

IV. Examination Procedures for Information Security Program

- OCC released the examination procedures for reviewing compliance with information security Guidelines (OCC Bulletin 2001-35)
- Tailored, with less detailed procedures for community banks
- Tie together risk assessment and information security program policies

Examination Objectives

- Five substantive objectives
- Correspond to substantive requirements of the Guidelines

1

Does FI have information security program complying with Guidelines?

- Board approved written program?
- Useful performance reports back to Board?
- Do management and Board adequately oversee program?

Does FI have adequate and effective formal risk assessment process?

- How are vulnerabilities identified?
- Risk to entire customer information system been evaluated? Process for sensitivity-ranking information assets?
- Do evaluation personnel have sufficient expertise?

Does FI have adequate and effective formal risk assessment process? (cont'd)

- Prioritize risk exposure, create and execute mitigation strategy

Is the program adequate to manage and control risk?

- Do controls include the following, as appropriate?
  - Limiting physical and logical access to authorized persons
  - Encryption of customer data
  - System change control procedures
  - Detection of attacks/intrusion

Is the program adequate to manage and control risk? (cont'd)

- Do controls include the following, as appropriate? (cont'd)
  - Incident response activities planned
  - Business continuity planning
- Adequately trained staff?
- Controls regularly and independently tested in accordance with risk assessment?

How does FI oversee service providers?

- Due diligence in selection?
- Do vendor contracts require information security program per Guidelines?
- Monitoring service providers
  - Do contracts provide for sufficient reporting to allow evaluation of performance and security?

How does FI oversee service providers? (cont'd)

- Do contracts provide for sufficient reporting to allow evaluation of performance and security?
- Does **FI** review and act on reports?
- Does **FI** review financial condition of service provider?

Does FI have effective process to adjust program?

- Procedures to adhere to Guidelines? Changes can include:
  - Technology changes
  - Information sensitivity
  - Threats
  - Changes to business arrangements, customer information systems

Does FI have effective process to adjust program? (cont'd)

- Has appropriate expertise been applied to decision whether to change program?
- Program changes implemented timely in a controlled manner?